

Cyber Security Tips

1

Good password management is key. Use a mix of upper and lowercase characters, symbols, and numbers in your password. Also, you shouldn't share your password with others, and you should change your password frequently.

2

Be careful of what you share on social media. Many of the things we share online can be used to gain information that can help someone gain access to your personal information.

3

Keep your software up to date. Software developers release patches and updates to help secure and protect their users, so you should always install the most recent updates.

4

Disable Bluetooth connectivity on your devices unless you are actively using it. Criminals can use Bluetooth to infect your devices.

5

Sensitive browsing, such as banking, shopping, or anything that involves personal information should only be done on a device you own, on a network you trust, such as your home. Never enter sensitive personal information on a public computer or internet connection.

6

Always check website addresses for the padlock and <https://> to ensure you're on a secure site, especially if you are entering personal information.

7

Be cautious when opening attachments or clicking links in emails. If it's unexpected or suspicious, don't click it. Remember, government agencies and reputable businesses will not contact you via email requesting sensitive information!

8

Never send personal or financial information over email, especially on a public Wi-Fi connection.

9

Be cautious about where you provide your email. Never enter your email address into a pop-up window or site you don't trust.

10

Don't click the "Unsubscribe" link or in spam emails or reply to them. Clicking the link will confirm to the spammer that your email is active and can open the door to more frequent attacks.